Awareness raising campaign for SMEs

Guidance on Legal Bases

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

An Coimisiún um Chosaint Sonraí Data Protection Commission

Croatian Personal Data Protection Agency azop Agencija za zaštitu osobnih podataka

VUB VRIJE UNIVERSITEIT BRUSSEL

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S RIGHTS, EQUALITY AND CITIZENSHIP 2014-2019 PROGRAMME UNDER GRANT AGREEMENT N°874524.

Contents

Overview

One of the first questions which organisations involved in processing personal data ('controllers') should ask themselves before undertaking the processing is "*What is my reason or justification for processing this personal data?*" This is of key importance because any processing of personal data is only lawful where it has what is known as a 'legal basis'. Article 6 of the General Data Protection Regulation (GDPR) sets out what these potential legal bases are, namely: consent; contract; legal obligation; vital interests; public task; or legitimate interests.[1]

Article 6 GDPR, lawfulness of processing;

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

- **a)** the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- **b)** processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- **c)** processing is necessary for compliance with a legal obligation to which the controller is subject;
- **d)** processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- **e)** processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- **f)** processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

All controllers need to determine which legal basis they are relying on in order to ensure that any processing they undertake is lawful. There is **no hierarchy** or preferred option within this list, instead each instance of processing should be based on the legal basis which is **most appropriate** in the specific circumstances.

Controllers should be aware that there may be different legal bases applicable where the same personal data are processed for more than one purpose. Further, it is important to note that **'consent',** whilst perhaps the most well-known, is **not the only legal basis** for processing – or even the most appropriate in many cases.

Article 6 GDPR also sets out that countries can introduce laws at a national level to further govern or adapt the requirements regarding legal basis, as has been done in the Irish Data Protection Act 2018 ('the 2018 Act').[2] The GDPR also allows that where certain conditions are met controllers may process personal data for purposes other than those for which they were originally collected, as is discussed further below under the heading 'Further Processing'.

The aim of this guidance is primarily to assist controllers in **identifying the correct legal basis** for any processing of personal data which they undertake or plan to undertake – and the

[1] See also, Recitals 39 and 40 GDPR; Recital 39 setting out that any processing of personal data should be lawful and fair, and Recital 40 further clarifying that in order for processing to fulfil that lawfulness requirement, personal data must be processed according to one of the legal bases.

[2] See, for example, section 38 on processing for a task carried out in the public interest or in the exercise of official Authority, or section 42 on processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

obligations which go with that legal basis. Additionally, this guidance should assist those individuals whose personal data may be processed ('data subjects') in identifying whether the processing of their personal data is lawful, and, as part of that, what the legal basis for that processing may be.

This guidance primarily focuses on the legal bases for processing covered by the GDPR; however, certain controllers may also process personal data which falls outside of the scope of the GDPR, and instead falls under the scope of the **Law Enforcement Directive (LED)** (and Part 5 of the 2018 Act, which transposes that Directive into Irish law). The prerequisites for processing personal data under the LED will also briefly be discussed below, under the heading 'Law Enforcement'.

Data Subject Rights

Some of the specific rights granted to data subjects under the GDPR only apply where processing is justified by particular legal bases. The table below gives a general outline of which rights could be applicable when personal data are processed under the different legal bases.

	Right of Access	Right to Rectification	Right to Erasure	Right to Restriction	Right to Portability	Right to Object
Consent	✓	✓	✓	✓	✓	~ Can withdraw consent
Contract	✓	✓	✓	✓	✓	✗
Legal Obligation	✓	✓	✗	✓	✗	✗
Vital Interests	✓	✓	✓	✓	✗	✗
Public Task	✓	✓	✗	✓	✗	✓
Legitimate Interests	✓	✓	✓	✓	✗	✓

It should also be kept in mind, however, that there can be other requirements or limitations regarding some of the data subject rights listed above, but, as a first step, controllers should consider which rights might be applicable in the first place when assessing their data protection obligations. Additionally, individuals always have the right to object to the processing of their personal data for the purposes of direct marketing, regardless of which legal basis applies.

Controllers may consider the question of which rights are applicable under which legal bases when assessing which legal basis is appropriate for a particular processing purpose, but **should not engage in selective application** of legal bases to reduce their compliance burden and **decrease the level of protection** for data subjects.

Principles of Data Protection

Having a legal basis is just one of the considerations controllers need to keep in mind when assessing the lawfulness of any processing of personal data they are undertaking. Controllers should also ensure that any processing **complies with the principles of data protection** laid out in Article 5 GDPR, namely: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality (security); and accountability.

Compliance with these fundamental principles of data protection is the first step for controllers in ensuring that they fulfil their obligations under the GDPR, and will also help controllers ensure they have a valid legal basis for any processing they undertake.

The principle of **lawfulness, fairness, and transparency** is of particular relevance to the question of legal basis, as having a valid legal basis is one of the key ingredients necessary for processing to be 'lawful'. As discussed further below, under the heading 'Transparency', controllers will also need to provide individuals with clear and transparent information about the purpose, or purposes, of processing their personal data and the legal basis, or bases, for doing so.

The legal basis for processing personal data will be closely tied to the purpose of that processing, and thus the principle of **purpose limitation** will play an important role in ensuring that processing has a valid legal basis. Personal data should only be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data.

As with the principle of purpose limitation, the principle of **data minimisation** will play an important role in assessing exactly what processing is justified by a particular legal basis, as well as the question of **'necessity'**, which is a key element of most legal bases. Processing of personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. Personal data which are processed beyond these limits, may not have a valid legal basis.

As part of data minimisation, controllers should also ensure compliance with the principle of **storage limitation**, to ensure personal data is only be kept in a form which permits identification of data subjects for as long as is necessary for the purposes for which the personal data are processed. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.

Ultimately, the controller is responsible for, and must be able to demonstrate, their compliance with all of the principles of data protection, in line with the **principle of accountability**. Controllers must take responsibility for their processing of personal data and how they comply with the GDPR, and be able to demonstrate (through appropriate records and measures) their compliance, in particular to the DPC.

Further information on these principles can be found in the guidance on the principles of data protection on the DPC website.

Transparency

As discussed above, controllers need to ensure that they are transparent about the processing they undertake, to ensure their compliance with the first principle of data protection, namely that all processing must be lawful, fair, and transparent.

It should be transparent to individuals that personal data concerning them are collected, used, consulted, or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information or communication relating to the processing of those personal data be **easily accessible and easy to understand**, and that clear and plain language be used.

Furthermore, as part of compliance with their **transparency obligations** under Articles 13 and 14 GDPR, controllers should ensure they provide data subjects with information including "*the purposes of the processing for which the personal data are intended as well as the legal basis for the processing*".

Providing clear and transparent information on the purpose, or purposes, of processing personal data as well as the legal basis, or bases, by which that processing is justified is of paramount importance, to ensure that individuals are able to easily identify the legal basis upon which a controller is relying, so that they can assess the lawfulness of the processing of their personal data.

Necessity

As evident from the text of Article 6 GDPR itself, most of the legal bases, apart from 'consent', only provide a justification for processing where it is 'necessary' for a particular purpose; for example, where it is "necessary for the performance of a contract", or "necessary in order to protect [...] vital interests". Exactly what processing is necessary to achieve a given purpose will vary from case to case, depending on the exact circumstances, and controllers will need to limit processing to that which is needed for an explicit purpose, in line with the principle of purpose limitation. These and other basic rules and considerations need to be taken into account when controllers are assessing the necessity and lawfulness of their processing activities.

As mentioned above, the Article 5 principle of 'data minimisation' also requires that personal data be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". The requirement of data minimisation also applies to processing undertaken on the basis of consent. Therefore, to comply with both the principles of data protection, as well as the lawfulness requirements of Article 6, controllers must ensure that any processing they undertake meets the test of necessity.

The concept of necessity has an independent meaning in European Union law, which must be interpreted in a way which reflects the objectives of data protection law. The concept of necessity is generally interpreted strictly by the Court of Justice of the European Union (CJEU), given that derogations or limitations on data protection rights are to be interpreted strictly. For example, in the Rīgas case, the CJEU stated that "[a]s regards [...] the necessity of processing personal data, [...] derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary...".

Necessity entails that processing should be a reasonable and proportionate method of achieving a given goal, taking into account the overarching principle of data minimisation, and that personal data should not be processed where there is a more reasonable and proportionate,

and **less intrusive way** to achieve a goal. In the Schecke case, the CJEU held that, when examining the necessity of processing personal data, the controller needed to take into account alternative, less intrusive measures, and any interference with data protection rights arising from the processing in question should be the least restrictive of those rights. In general, to satisfy the necessity test, there ought to be **no equally effective available alternative** .[3]

In light of the above, controllers should make sure that any processing of personal data which they undertake, or propose to undertake, is **more than simply convenient** for them, or potentially **useful**, or even just the **standard practice** which they or their industry have used up to now. Instead, controllers should ensure that each processing operation is necessary as a specific and proportionate way of achieving a transparent stated purpose or goal, which could not reasonably be achieved by some other less intrusive means, or by processing less personal data. Controllers also need to keep in mind that for more intrusive processing, a stronger justification will be required.

Special Categories of Personal Data

The processing of certain sensitive types of personal data, known as 'special categories' of personal data, is **prohibited, except for in limited circumstances**, as set out in Article 9 GDPR. Such processing requires both a legal basis under Article 6 GDPR, as well as meeting one of the conditions of Article 9 (such as explicit consent or protection of vital interests) which allow such data to be processed.

The additional requirements to process special categories of personal data under Article 9 GDPR are not within the scope of this guidance, but controllers should be aware of the **necessity to comply with both requirements** when processing such special categories of personal data.

[3] CJEU, Joined Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk*, para 88.

Consent

> **"the data subject has given consent to the processing of his or her personal data for one or more specific purposes"**
>
> **Article 6(1)(a) GDPR**

As mentioned above, 'consent' is probably the legal basis with which both data subjects and controllers are most familiar, and may even be seen as the 'go-to' by many controllers when assessing what legal basis they should be relying upon for various data processing operations. However, contrary to the high profile and popularity of consent as a legal basis, it is not necessarily a more appropriate legal basis than any other and – as with any legal basis – the DPC recommends that controllers **carefully consider** whether it is the **most appropriate** legal basis and the **requirements and obligations** attached to the reliance on consent as a legal basis for processing personal data.

In this section we will outline the definition of consent and what exactly constitutes consent under the GDPR, as well as the importance of a controller being able to demonstrate that a data subject has consented to processing, the 'conditions for consent' under Article 7 GDPR, and the requirements regarding the withdrawal of consent.

For a more detailed analysis of the notion of consent under the GDPR, we recommend consulting the Article 29 Working Party Guidelines on Consent.[4]

What Constitutes Consent?

The **definition of consent** is found in Article 4(11) GDPR, and sets out that consent must be freely given, specific, informed, and unambiguous, as well as that it must be made by way of a statement or 'clear affirmative action'. It is important to note that the definition of consent as required under the GDPR has been changed somewhat from that which was present in the previous legislation, the 'Data Protection Directive' (95/46/EC).

[OLD] Data Protection Directive definition of consent:	**[NEW] GDPR definition of consent:**
"any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed"	"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"

[4] These guidelines were prepared by the Article 29 Working Party, which has now been replaced by the European Data Protection Board (EDPB), in advance of the GDPR coming into effect on 25 May 2018. The EDPB has subsequently endorsed these guidelines.

Recital 32 GDPR gives some helpful guidance as to what may constitute valid consent, which highlights the differences between the definitions set out above. It restates that for consent to be valid it should be given through 'a **clear affirmative act**' and should be **'unambiguous**', giving examples such as ticking a box when visiting a website, choosing technical settings for a website or app, or another form of statement or conduct which clearly indicates the individual's acceptance of the proposed processing; it is specifically stated that "***[s]ilence, pre-ticked boxes or inactivity*** *should not therefore constitute consent*." The Article 29 Working Party guidance also stated that:

> The GDPR does not allow controllers to offer pre-ticked boxes or opt-out constructions that require an intervention from the data subject to prevent agreement (for example 'opt-out boxes').

In cases where consent is given by electronic means**,** the mechanism for obtaining consent should be **clear, concise and not unnecessarily disruptive** to the use of the service for which it is provided; however, it may be necessary that a consent request interrupts the service to some extent to ensure the consent is informed, clear, and effective. Where consent is given in the context of a written declaration which also concerns other matters, the request for consent must be presented in a manner which is **clearly distinguishable** from the other matters, per Article 7(2) GDPR.

One of the most important factors in obtaining valid consent is ensuring that the consent to processing is **specific and informed**. Controllers should make particular efforts in how they present both information and choices to data subjects, so that they can be certain – and later demonstrate – that the individual has understood to exactly what they are being asked to consent. For example, where processing has multiple distinct purposes**,** an individual should give specific and informed consent to each of them.

For consent to be informed, as noted in Recital 42 GDPR, individuals should be aware at least of the identity of the controller and the **purposes of the processing** for which the personal data are intended. Controllers should also be aware that consent cannot be obtained through the same action as agreeing to a contract or accepting general terms and conditions of a service,[5] as a blanket acceptance of this type would not be seen as a clear, affirmative, and specific action to consent to the processing.

Consent must also be **'freely given'** and Recital 43 provides guidance on how this requirement is to be interpreted, noting that consent should not be relied upon as a legal basis where there is a **clear imbalance** between the individual and the controller. Such a situation would bring into question whether the individual's choice to consent was in fact 'free'. This could occur in particular where the controller is a public authority, or employer,[6] or otherwise in a position of power, and it is therefore unlikely that consent was freely given in the context of that relationship.

Similarly, consent will be presumed not to have been freely given if the data subject was not given the opportunity **consent separately** to distinct processing operations for different purposes. As noted above, controllers should also be wary when using consent in conjunction with a contract, because if the performance of that contract is made dependent on the individual providing consent to certain processing despite it not being necessary for such performance the consent will be invalid.

---

[5] See Article 7(3) GDPR and the Article 29 Working Party Guidance, page 16

[6] It should be noted, however, that Recital 155 GDPR does indicate that Member State law or collective agreements, may provide for specific rules on the processing of employees' personal data in the employment context, in particular for the conditions under which it may be processed on the basis of employee consent.

Children's Consent

The GDPR contains a number of specific protections for children's data protection rights, including the specific provisions in Article 8 GDPR, setting out the conditions applicable to obtaining a **child's consent** in relation to **information society services**.[7] It should be noted, however, that consent is not the only possible legal basis for the processing of children's personal data, and controllers should assess on a case-by-case basis which is the most appropriate legal basis for any proposed processing.

Where such services are offered directly to a child, and the controller seeks to rely on consent as a legal basis, the child's must be at least 16 years old to consent independently, or, if the child is younger, the holder of parental responsibility must have given or authorised the consent. Whilst Article 8(1) does allow for Member States to set the age at a lower level (between 13 and 16), the 2018 Act has maintained the age cut-off for consent to such services at 16 years old in Ireland.

In cases involving children under 16, controllers must make **reasonable efforts to verify** that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

Demonstrating Consent

Being able to actually **show that a data subject has consented** to specific data processing is a key obligation on controllers who rely on the legal basis of consent, as set out in Article 7(1) GDPR, as well as a requirement of the principle of accountability. The controller should be able to demonstrate that the data subject has given consent to the processing, and if consent is given in the context of a written declaration which also covers other matters, safeguards should ensure that the data subject is aware to what, and the extent to which, they are giving consent.

If a controller utilises a **declaration of consent** which they have pre-formulated, it should be provided to the data subject in an intelligible and easily accessible form, using clear and plain language and it shouldn't contain any unfair terms.[8]

Demonstrating consent is not just a matter of showing a choice at a single point in time and controllers should consider ensuring that consent is valid as an **ongoing and dynamic obligation**, not a one-off event. Controllers should review consent and seek renewed consent if any relevant details of the processing operation or purpose changes (meaning the original consent may no longer be truly 'informed') or to consider seeking renewed consent at certain intervals if appropriate.

A useful option for many controllers, particular those providing online services, is to provide preference-management tools like **privacy dashboards** which allow data subjects to easily access and manage their consent settings.

Withdrawing Consent

The ability to **withdraw consent at any time** after granting it is a key component of the concept of consent under Article 7(3) GDPR, and thus controllers need to be certain that they can

[7] 'Information society services' are defined (in DIRECTIVE (EU) 2015/1535) as "*any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services*", and generally covers most online services, even where the 'remuneration' or funding is not directly paid for but otherwise supported – such as by advertising. This generally covers, websites, apps, search engines, and online service and content providers

[8] Per Recital 42 GDPR and Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts

facilitate the withdrawal of consent by individuals if they rely on this legal basis. If withdrawing consent would be highly impractical, impossible, or make the purpose of the processing unworkable, then controllers should consider whether another legal basis may be more appropriate in the circumstances, or whether there is a legal basis for the processing at all.

The withdrawal of consent will not, however, affect the lawfulness of processing based on that consent before it was withdrawn. Controllers must also ensure that withdrawing consent is **as easy as granting** it. For example, if the process for granting consent was a simply one-step process, then withdrawing consent should be a similarly simple one-step process. Controllers should endeavour to enable data subjects to withdraw their consent using the same or a similar method as when they granted it.

Data subjects have the right to withdraw consent **'at any time'**, therefore providing only limited or hard to access options to 'opt-out' or withdraw consent will not fulfil this obligation; the data subject should be able to withdraw consent easily, at any time they choose, on their own initiative.

Recital 42 GDPR notes that consent will also not generally be regarded as freely given if the data subject has no genuine or **free choice** or is unable to **refuse or withdraw** consent **without detriment**.

Contract

> **"processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract"**
>
> **Article 6(1)(b) GDPR**

The legal basis of 'contract' (also referred to as 'contractual necessity' or 'contractual performance') is another relatively commonly utilised legal basis for the processing of personal data, in contexts where there is a **contractual relationship** between the **data subject and the controller**. Article 6(1)(b) and Recital 44 GDPR set out that processing may be lawful where necessary for performing or initiating a valid contract.

Controllers need to be aware that to rely on a contractual legal basis for processing personal data it isn't sufficient for the processing to just be somehow related to the contractual relationship, instead it must go further and be '**necessary for the performance**' of that contract – i.e. objectively necessary to carry out the contract. Alternatively, this legal basis may be relied upon where the processing is necessary to **take steps** leading towards a contract, where the data subject has requested the controller do so, as discussed in more detail below.

As set out in the wording of Article 6(1)(b) GDPR, controllers need to be aware that this legal basis can only apply to **contracts between the actual data subject and the controller**, and not to processing of personal data for the purpose of performing a contract between a controller and a third party. Thus, a controller cannot use a contract between themselves and another service provider or advertising partner as the legal basis for the processing of a data subject's personal data, just because the processing would be necessary to perform that contract – as the data subject is not a party to that contract. Thus, this legal basis would not apply in the **absence of a direct contractual relationship** with the data subject concerned.

Prior to Entering into a Contract

The wording of Article 6(1)(b) GDPR reflects the fact that preliminary processing an individual's personal data may be necessary before entering into a contract with the controller, in order to facilitate concluding a contract, such as the processing of personal details by an insurance company where a data subject has **asked for a quote**, with a view to potentially entering into a contract of insurance.

In an online context, this may be of relevance in situations where, for example, a data subject provides their postal address to see if a particular service provider operates in their area, or processing which is carried out as part of a registration process for an online service. This idea of preliminary processing **could not cover unsolicited marketing** or other processing which is carried out solely on the initiative of the controller, or at the request of a third party, as this isn't done at the request of the actual data subject.

Example

An online service provider creates a function that allows its users to invite non-members to join the service. Where such an invite is sent, the company collates all the information it holds on the person invited (the invitee) in order to assemble a preliminary profile of their connections to other users, to encourage them to sign up. Since the invite has been sent at the request of a third party (the original user sending the invite), the data subject profiled (the invitee) has not asked the controller to take any steps, and therefore the company cannot legitimately rely on Article 6(1)(b) as its basis for this pre-contractual processing.

Necessity and Performing Contracts

The concept of what precisely is 'necessary' will ultimately will depend on the **circumstances of each case** and the wording, nature, and circumstances of the contract. As mentioned above, controllers need to ensure that processing is **objectively necessary and a proportionate** way to perform the contract, taking into consideration other potentially less intrusive means of achieving the purpose of the processing**.** Controllers should also consider the general guidance on the application of the principle of necessity to legal bases, set out above under the heading 'Necessity', when assessing what is necessary for the performance of a contract.

In some cases, written contractual terms may clearly specify that processing of personal data is required as an element of performance of the contract. However, it is not required for the purposes of Article 6(1)(b) that each granular processing operation must be specified in contractual terms. In many cases, processing which is necessary for the performance of a contract will not be expressly stated in contractual terms between the parties, and instead must be considered in the wider **context of the agreement** entered into, including an assessment of what is **reasonably necessary** in order to perform the underlying agreement.

This does not obviate the controller's obligations regarding the **principles of transparency**, in particular under Article 13 GDPR, to ensure that the data subject is **aware of both the types of processing operations and purposes** of processing which will be undertaken with their personal data. This includes the express obligation under Article 13(2)(e) to provide information (at the time personal data are obtained from a data subject) on whether the provision of personal data is a contractual requirement.

Example

A customer goes into a clothes shop to buy a new jacket. The shop doesn't currently have their size is stock, but agrees to order it and contact the customer once it is ready. The customer pays for the jacket and provides their contact details so they can be contacted once it has arrived.

The shop then uses the contact details and purchase information to create a loyalty card and online profile for their customer to use, which they inform them about when they come back into the shop, much to the customer's surprise.

In this case, the terms of the contract of sale between the parties does not support the conclusion that the creation of a loyalty card or profile is reasonably necessary to perform the contract as entered into.

Where Contract Is Limited as a Legal Basis

One consideration, which is beyond the scope of this guidance, that controllers need to take into account when considering a contractual legal basis for processing personal data, is the need to comply with the various other laws which govern contractual relationships. In particular, a data subject may be a child or otherwise have **limited or no capacity to enter into a contract**. Likewise, there may be other **contract or consumer law** considerations which mean that certain contracts or contractual clauses are invalid.

Before a controller can rely on contractual performance as a legal basis for processing personal data, they **must satisfy** themselves that there is a **valid underlying contract**, and that any clause(s) the performance of which necessitate the processing of personal data are valid and enforceable.

As discussed above, where the processing of personal data is not actually necessary to perform the contract between the data subject and controller, then controllers will have to assess whether the processing may be **based on another legal basis**, or whether any legal basis is available at all. However, as noted above (under the heading 'Consent'), controllers should not seek to rely on consent as a legal basis where they make that act of consent a condition of the contract.

If processing of sensitive **'special category' data** is necessary as part of performing the contract, controllers will also need to **identify a separate exception** to the general prohibition of processing such data, because contractual necessity alone does not fulfil the requirements of Article 9 GDPR. Thus, as with all processing of such special category data, the controller will need both a legal basis – in this case, necessary for the performance of a contract – as well as fulfilling a condition under Article 9(2) which allows for the processing that type of personal data – such as the fact that the data have been 'manifestly made public' or the processing is necessary to establish, exercise, or defend a legal claim.

Legal Obligation

> **"processing is necessary for compliance with a legal obligation to which the controller is subject"**
>
> **(Article 6(1)(c) GDPR)**

This legal basis, also known as '**compliance with a legal obligation**', is likely to be the appropriate legal basis in cases where controllers are obliged to process the personal data to comply **with EU or Irish legislation or the common law**. Similarly to reliance on contract as a legal basis, to rely on a legal obligation a controller must assess whether processing is actually '**necessary' in order to comply** with that obligation. If you can reasonably comply without processing the personal data, reliance on this basis will not be appropriate.

Article 6(1)(c) describes this legal basis as one where the processing is necessary for compliance with an obligation to which the controller is actually subject. In Article 6(3) it is clarified that such an obligation must be grounded on and emerge from either **EU or Irish law** (or the law of another Member State, where applicable).

There does not have to be a legal obligation specifically requiring the exact processing activity which the controller is going to undertake; however, controllers should ensure that the **overall purpose** of the processing of the personal data is to comply with a legal obligation which has a **sufficiently clear basis** in either common law or legislation.

In line with both the principles of **transparency** as well as a**ccountability**, controllers should ensure that they are able to **identify the specific law** which they believe constitutes the legal obligation for which the processing is necessary. As part of demonstrating accountability and compliance, controllers may refer to specific provisions in legislation, case law, official or governmental advice or guidelines, or other official guidance which sets out the obligations to which the controller might be subject.

What Constitutes a Legal Obligation?

As set out above, a legal obligation must be laid down by EU or national law. Recital 41 GDPR further clarifies that any law which might ground a legal obligation in this context does not only cover a legislative act adopted by a parliament (i.e. legislation), as the GDPR acknowledges the diverse constitutional orders of the Member States.

Thus, a legal obligation may be grounded on **primary legislation** (such as an Act), **secondary legislation** (such as a statutory instrument, or 'SI'), or some **common law** requirement.

The GDPR does note that any such a law should be **clear and precise** and its application should be '**foreseeable** to persons subject to it', in accordance with the case-law of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR).

There does not need to be a law that clearly obliges controllers to engage in a specific act of data processing, but rather a law or obligation may be the **basis for several processing operations**, as long as those processing operations are **actually necessary** to comply with that obligation. As set out in both Article 6(3) and Recital 45 GDPR, any such law which grounds a legal obligation should at least make clear the purposes of any processing which is undertaken to comply with

that obligation, and must meet an objective of **public interest**, being **proportionate** to a legitimate aim or goal which is being pursued.

What is Necessary to Comply with a Legal Obligation?

The concept of **'necessity'** is also a key component of the legal basis of 'compliance with a legal obligation', as the data processing must be actually **necessary in order to comply** with the obligation. In most cases it should be clear from the law in question whether the processing is actually necessary for compliance.

Processing in order to comply with a legal obligation must be a **reasonable and proportionate way of achieving** that compliance. For example, a controller should not rely on compliance with a legal obligation as a legal basis for processing if they have a **discretion** over whether to process the personal data, or if there is another more reasonable and proportionate, and **less intrusive** way to comply with the obligation. This is in line with the principle of **data minimisation**, in that the processing of personal data should only be undertaken in a limited way, where relevant and necessary to achieving the purpose of the processing.

As is the case with other legal bases which involve the concept of necessity, the extent of what precisely is 'necessary' for compliance with a legal basis will ultimately depend on the **circumstances of each case** and the nature of the legal obligation. In the *Huber* case,[9] the CJEU stated, in the context of a register of foreign nationals, that processing could only be considered 'necessary' if it contained **only the data which were necessary** for the application by the authorities of that legislation and contributed to the **more effective performance** of the legislative obligations.

[9] CJEU, Case C-524/06, *Heinz Huber v Bundesrepublik Deutschland*, 18 December 2008, para 62.

Vital Interest

> **"processing is necessary in order to protect the vital interests of the data subject or of another natural person"**
>
> **(Article 6(1)(d) GDPR)**

Processing personal data to protect the vital interests of an individual is a less commonly used legal basis, but is nevertheless important to consider in **certain specific situations** where other legal bases are not appropriate. As with certain other legal bases, controllers should consider whether the processing is in fact **necessary to achieve the goal** of protecting vital interests. Controllers are most likely to rely on this legal basis where the processing of personal data is needed in order to **protect someone's life**, or mitigate against a serious threat to a person, for example a child or a missing person.

Vital interests may be an appropriate legal basis in atypical circumstances, where none of the other legal bases clearly apply. For example, where sensitive special category personal data is concerned, **such as health data** – potentially in an **emergency situation** – vital interests may provide both a legal basis under Article 6, but also an exception from the prohibition of processing such data under Article 9 GDPR.

Many cases in which the protection of vital interests is relied upon as a legal basis for processing are likely to involve special category health data, and **Article 9(2)(c) GDPR** allows for processing such data where necessary to protect someone's vital interests; but, this only applies if the data subject is physically or legally incapable of giving consent.

Example

Paramedics are called to a residential care facility to assist a seriously ill resident, who is unconscious when the paramedics arrive. The medical history and other relevant health data of the resident may be shared with the paramedics as it is necessary to do so to protect their vital interests – even where, for example, the resident has not previously consented to the sharing of this data for such purposes.

Nevertheless, this legal basis will **not apply to all situations** concerning the health or treatment of a data subject, but only where the processing is necessary to protect vital interests. As such, it is **less likely** that this legal basis would apply **outside of an emergency situation**, for instance where medical care has been planned in advance.

Whose Vital Interests Are Relevant?

It should be noted that the legal basis of vital interests under the GDPR can apply to the processing of a data subject's personal data to protect ***their*** **vital interests**, but also potentially to the processing of that data subject's personal data to protect the **vital interests of *another individual*** – although the circumstances in which this is likely to be the case are more limited.

Nevertheless, processing of a data subject's personal data to protect the vital interests of another may happen, for example, where it is necessary to process a **parent's personal data** to

protect the **vital interests of their child**. Processing of personal data based on the vital interest of another individual should in principle take place only where the processing manifestly cannot be based on another legal basis.

Reliance on vital interests as a legal basis is **less likely** to be appropriate for **larger scale processing** of the personal data of multiple individuals – it's more likely to be appropriate in individual emergency situations. Nevertheless, Recital 46 GDPR does suggest that vital interests could be an **appropriate** legal basis for **larger scale processing on humanitarian grounds** in the context of a situation such as an epidemic or disaster.

Necessity and Emergency Situations

For vital interests to be relied upon as a legal basis, the intended processing must actually be objectively ***necessary* in order to protect the vital interests** of the data subject or another individual – meaning that it must be a **reasonable and proportionate way of achieving** protecting those interests. If a controller can reasonably protect a data subject's vital interests in another, less intrusive way, it is unlikely that vital interests will be an appropriate legal basis.

In line with the principle of **data minimisation**, processing of personal data should only be undertaken in a limited way, where relevant and necessary to achieving the purpose of the processing. To ensure accountability, controllers should record their reasoning as to why they thought it necessary to process personal data to protect the vital interests.

A with all legal basis which include a test for necessity, the extent of what precisely is 'necessary' to protect a data subject's vital interests will ultimately depend on the **circumstances of each case** and a the context will have to be taken into account particularly in emergency situations where the controller honestly believed that the processing was necessary to protect vital interests. Where a controller is likely to be involved in such situations, some degree of **scenario planning** should be undertaken so that clear processes, including on how to handle personal data, are in place.

What are 'Vital Interests'?

Recital 46 GDPR further elaborates on the kinds of situations in which vital interests may apply, namely where it is "*necessary to protect an interest which is essential for the life of the data subject or that of another natural person*" (i.e. a living individual). Thus, vital interests can be understood as **interests *essential* for the life of a data subject** – mainly covering life-threatening situations, but potentially situations which very seriously threaten the health or fundamental rights of an individual.

For these reasons, and as alluded to above, **most cases** in which vital interests are the appropriate legal basis will involve **medical or healthcare situations**, including people in vulnerable mental states, and will often involve sensitive, special category data. The protection of the actual life of the data subject or another individual is most likely to be the vital interest which is protected by the necessary processing of personal data.

When considering which legal basis is most appropriate, controllers should note that certain types of processing **may serve** both important grounds of **public interest** as well as the vital interests of the data subject as for instance when processing is necessary for **humanitarian purposes**, including for monitoring epidemics and their spread or in situations of humanitarian emergencies.

Public Task

> **"processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"**
>
> **(Article 6(1)(e) GDPR)**

This legal basis is likely to apply to a more limited sub-set of controllers, where it is necessary for them to process personal data to carry out a task in the public interest, or exercise their official authority.

The GDPR makes clear, at the end of Article 6(1), that **public authorities cannot rely on the legal basis of 'legitimate interests'** to justify the processing of personal data which is carried out in performance of their tasks. In the past, some of this type of processing may have been done on the basis of legitimate interests, but public authorities now need to consider whether the appropriate legal basis is the performance of a task in the public interest or the exercise of official authority.

Article 6(3) GDPR also sets out that where processing is based on this legal basis, it should be **grounded on EU or national law**, which meets an objective or public interest and is **proportionate and legitimate** to the aim pursued. Thus, a controller may rely on this legal basis if it is necessary for them to process personal data either in the exercise of **official authority** (covering public functions and powers as set out in law) or to perform a **specific task** in the **public interest** (as set out in law).

This legal basis is **most relevant to public authorities**, but could also potentially be relied upon by any controller which in some way exercises official authority or carries out a task in the public interest. There does **not need to be a specific legal power** to process personal data attributed to that controller, but their underlying task, function or power must have a **clear basis in EU or Irish law**, **including common law**. Recital 41 GDPR makes it clear that the law which grounds the task, function, or power should be clear and precise and its application should be **foreseeable** to those affected by it, in accordance with the case-law of the CJEU and ECtHR.

As mentioned in Recital 45 GDPR, a particular law may be sufficient to serve as the grounds for several processing operations where the processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority. The GDPR also notes that it is for **EU or national law to determine the purpose of processing** in such cases.

Controllers should also note the related point that processing of personal data relating to criminal convictions and offences pursuant to one of the legal bases in Article 6(1) GDPR can only be carried out under the control of official authority or when the processing is authorised by EU or national law, which provides for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive **register of criminal convictions** shall be kept **only under the control of official authority**.

What Kinds of Tasks are in the Public Interest?

Examples of areas in which a task may be carried out in the public interest are given in Recital 45 GDPR, including **health purposes** such as **public health** and **social protection** and the

management of **health care services**. Recital 55 GDPR notes that the processing of personal data by official authorities for the purpose of **achieving the aims of officially recognised religious associations**, as laid down by constitutional law or international public law, may be considered to be carried out on grounds of public interest.

Section 38 of the 2018 Act contains further detail on processing for a task carried out in the public interest or in the exercise of official authority in Irish law. It states that processing of personal data shall be lawful to the extent that such processing is **necessary and proportionate** for (a) the performance of a **function** of a controller **conferred by or under an enactment or by the Constitution**, or (b) the **administration** by or on behalf of a controller of any **non-statutory scheme**, programme or funds where the legal basis for such administration is a function of a controller conferred by or under an enactment or by the Constitution. Section 38 also contains details on processing for the purposes of preserving the Common Travel Area, and rules on how ministerial regulations can be made to provide further detail on tasks carried out in the public interest.

Section 42 of the 2018 Act sets out further rules regarding processing personal data for **archiving** purposes in the public interest, **scientific or historical research** purposes or **statistical** purposes, in accordance with Article 89 GDPR. It notes that where those purposes can be fulfilled by processing which does not permit, or no longer permits, identification of the individual data subjects, the processing of information for such purposes should be done in that manner.

Further, Recital 56 GDPR suggests that where the operation of the democratic system of the State, in the **course of electoral activities**, requires that political parties compile personal data on people's political opinions, the processing of such data may be permitted for reasons of public interest. However, this only applies provided that **appropriate safeguards** to protect data subject rights are established. Section 48 of the 2018 Act reiterates that processing of personal data revealing political opinions for electoral activities and functions of the Referendum Commission is lawful.

Controllers should also consider whether this legal basis is appropriate in cases where processing is necessary for **humanitarian purposes**, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters, as set out in Recital 46 GDPR (which also notes that vital interests may be an appropriate legal basis appropriate in such cases).

Necessity, Proportionality, and Minimisation

Controllers relying upon this legal basis need to ensure that the processing of the personal data of the data subject must actually be ***necessary*** **in order to carry out the task in the public interest or exercise official authority**. As is the case of other legal bases which involve the concept of necessity, the extent of what precisely is 'necessary' to carry out the task in the public interest or exercise official authority will ultimately depend on the **circumstances of each case.**

For processing to be necessary to carry out a task in the public interest or exercise official authority, it must be a **targeted, reasonable, and proportionate way** of doing so. If a controller can reasonably achieve these purposes in another, less intrusive way, it is unlikely that they should process personal data under this legal basis, in line with the principle of **data minimisation**.

In particular, as public authorities have access to potentially very large amounts of personal data, it is imperative that they ensure both the **type and amount of personal data** processed are **adequate, relevant and limited** to what is necessary to achieve the stated purpose.

Which Controllers Can Rely on this Basis?

Recital 45 GDPR sheds some light on the question of which categories of controllers might rely on this legal basis, and in which circumstances. It notes that it is primarily for specific EU or national law to determine what kind of controller can perform a task carried out in the public interest or exercise official authority.

Most commonly, the controller is likely to be a **public authority** or another natural or legal person **governed by public law**, but might also include, where it is in the public interest to do so, controllers governed by private law, such as **professional associations**.

As noted above, **public authorities** are also likely to rely on this legal basis for many processing operations, as they are **explicitly prevented** from relying on the legal basis of 'legitimate interests' under Article 6(1) GDPR for processing 'in the **performance of their tasks**', and consent will not be an appropriate legal basis for processing operations where the data subject has no real choice to freely give consent (which may often be the case due to the imbalance of power between data subjects and public authorities).

As discussed below under 'legitimate interests', this does leave open the possibility for public authorities to rely on legitimate interests as legal basis for a reason other than performing their tasks as a public authority. The DPC's position is that the performance of the tasks of a public body relates to the substantive tasks of a public body, and thus, ancillary purposes, such as transparency, office management, or financial accountability, may be appropriate to carry out on the basis of legitimate interests in those contexts.

Legitimate Interests

> **"processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child"**
>
> **Article 6(1)(f) GDPR**

Legitimate interests is a **versatile and flexible** legal basis for the processing of personal data, which may apply in circumstances where processing operations do not fit neatly into any of the other legal bases; however, it also carries **heightened obligations** on controllers to balance the legitimate interests they are seeking to pursue with the **rights and interests of the data subject**.

Controllers who are assessing whether to process data under the legitimate interest legal basis should consider the three elements needed for this legal basis:

a) identifying a **legitimate interest** which they or a third party pursue;

b) demonstrating that the intended processing of the data subject's personal data is **necessary to achieve** the legitimate interest; and

c) **balancing** the legitimate interest against the **data subject's interests**, rights, and freedoms.

As such, legitimate interests is likely to be an appropriate legal basis in cases where controllers process data subjects' personal data in a way which they would **reasonably expect** and which would have a minimal impact on their privacy, by virtue of the nature of the processing or safeguards introduced. Where there would be a more than minimal impact on the data subject's privacy rights, or other rights, freedoms, or interests, it may still be possible to rely on this legal basis, but the legitimate interest being pursued by the controller would need to be a particularly compelling justification for processing.

In many ways, the legal basis of 'legitimate interests' may be due more consideration as a potential legal basis by controllers, as for many situations it both provides **flexibility** to data controllers but also requires them to specifically consider the **interests and rights** of the data subject and to ensure appropriate safeguards and protections are in place.

Article 6(1) GDPR actually specifically **restricts public authorities** from relying on the legal basis of legitimate interests if they are processing personal data 'in the **performance of their tasks'**. However, this does leave open the possibility for public authorities to rely on this legal basis for a legitimate reason other than performing their tasks as a public authority. The DPC's position is that the performance of the tasks of a public body relates to the substantive tasks of a public body (e.g. relating to the purpose for which the public body was established). Accordingly, ancillary purposes, arising, for example, from the status of a public body, such as transparency, office management, or financial accountability, may be appropriate to carry out on the basis of legitimate interests in those contexts.

What Kinds of Legitimate Interests Are Covered?

As set out in Article 6(1)(f) GDPR, the legitimate interests which ground reliance on this legal basis may either be *those of the controller* itself or the **interests of third parties**. The types of legitimate interests may include **commercial interests, individual interests, or broader societal benefits.** This legal basis is not limited to specific categories of relationship between controllers and data subjects (apart from the restriction regarding public authorities in performance of their task), thus it is open to controllers to consider the appropriateness of this legal basis in a **wide range of situations**.

A relevant legitimate interest could, for example, exist in various situations where there is a **'relevant and appropriate relationship'** between the data subject and the controller, as noted in Recital 47 GDPR. This might apply in situations such as where the data subject is a client or in the service of the controller. The existence of a legitimate interest requires careful assessment, including, in particular, whether a data subject can **'reasonably expect'** at the time and in the context of the collection of the personal data that processing for that purpose may take place.

The GDPR, at Recital 47, gives some more concrete examples of the kinds of interests which might constitute legitimate interests for this purpose, noting that the processing of personal data strictly necessary for the purposes of **preventing fraud** is likely to constitute such, and even that processing for **direct marketing** purposes may be regarded as carried out for a legitimate interest.[10] In both cases, particularly the latter, controllers will still need to carefully assess whether the purposes of their intended processing do in fact constitute a legitimate interest, as well as balancing this against the data subject's interests, as discussed in more detail below. Recital 47 also notes that a legitimate interest could exist where there is a 'relevant and appropriate relationship' between the data subject and the controller, such as where the **data subject is a client or in the service of the controller**.

Further, Recital 48 GDPR suggests that *"[c]ontrollers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data **within the group of undertakings** for internal administrative purposes*", and that this could include processing of clients' or employees' personal data. However, it does note that the general principles for the transfer of personal data to an undertaking located in a third country (outside the EU/EEA), in this context, remain unaffected, and controllers should still ensure full compliance with the requirements for such transfers.

Recital 49 GDPR also sets out in some detail the kinds of **network and information security considerations** which might constitute a legitimate interest for processing personal data, to the extent it is 'strictly necessary and proportionate' for those purposes. It lists as examples the ability of a network or an information system to resist accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems – including **preventing unauthorised access** to systems and **stopping 'denial of service'** attacks.

Necessity and Legitimate Interests

Once a legitimate interest has been identified, a controller must be able to show that the processing of personal data is actually necessary for the purpose of that interest. The necessity

[10] In many cases, consent will be required for electronic direct marketing, under regulation 13 of S.I. No. 336/2011 – the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 ('the ePrivacy Regulations'). However, where direct marketing falls outside the remit of the ePrivacy Regulations (such as postal marketing) or where the exception in regulation 13(11) applies, legitimate interests may provide a legal basis for such processing.

test requires controllers to demonstrate that the processing is a **reasonable and proportionate way of achieving their purpose**. If a controller can reasonably pursue these interests in another, **less intrusive way**, legitimate interests will not provide a legal basis for processing.

Therefore, when assessing whether processing is necessary for the purpose of pursuing a legitimate interest, controllers should consider whether the processing actually helps to further the identified interest, whether it is a reasonable and proportionate way to do so, and whether there are any less intrusive ways to achieve the same result.

In line with the principle of **data minimisation**, even where processing may seem necessary, controllers should ensure that the amount of data processed and extent of that processing is the minimum amount needed to achieve the stated purpose.

As is the case of other legal bases which involve the concept of necessity, the extent of what precisely is 'necessary' for the purposes of any legitimate interest will ultimately depend on the **circumstances of each case,** and will also be relevant to the consideration of the balancing of interests, as discussed below.

The Balancing Test

As mentioned above, a key component of this legal basis is that it may only be relied upon where the legitimate interests which are pursued by the controller or third party are **not overridden by the interests**, rights, and or fundamental freedoms of the **data subject**. As such, controllers need to undertake a **balancing exercise** when assessing whether the processing of personal data should take place under this legal basis. This exercise should, as noted in Recital 47 GDPR, take into consideration the **'reasonable expectations'** of data subjects, in the context of their relationship with the controller.

In particular, controllers should pay special attention and afford **extra protection to the interests or fundamental rights and freedoms** of the data subject where the data subject is a **child**, as specifically required in the wording of Article 6(1)(f) itself. The GDPR more broadly requires heightened levels of protection of children's data protection rights, which should be kept in mind by controllers when balancing these interests. Recital 38 GDPR, for example, notes that "*[c]hildren merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data*", and suggests this is particularly the case where marketing or profiling are concerned.

A large part of the balancing test undertaken by controllers should also be based on **common sense** and the **expectations of the data subject**: If a data subject would not reasonably expect this type of processing of their personal data, or if it would cause unjustified harm to their interests, rights, or freedoms, their interests are likely to override the legitimate interests upon which the controller is seeking to rely. Similarly, the greater the intrusion a certain processing operation has on the data protection rights of an individual, the greater the justification needed to ground that processing.

A balancing test is needed as a controller's interests will not always align with the interests of the data subject(s). However, where there is a conflict or tension between these interests it is not the case that processing can never take place, but rather the controller can only process the personal data where their interests provide a **clear and proportionate justification for the impact** on the individual.

Thus, where a controller is considering processing personal data based on legitimate interests, they should **ensure that they have undertaken the balancing test**, and are confident that the data subject's interests do not override those legitimate interests and that the personal data are only used in ways the data subject would reasonably expect – unless there is a very strong reason overriding these concerns. Further, they should take particular care to ensure protection of children's interests where there personal data are to be processed. Controllers should also be sure they have considered appropriate safeguards to reduce any negative impact, where possible.

Factors which should be considered as part of the balancing test include the **circumstances and context of each case**, in particular the nature of the personal data and the processing and the relationship between the controller and data subject, but **also data protection considerations** such as data minimisation, retention periods, safeguards in place, data protection by design and by default, and the existence of clear and accessible opt-out mechanisms.

In line with the **principle of accountability**, found in Article 5 GDPR, controllers should keep a record of the assessment they undertook to determine whether the legitimate interests were overridden by the interests, rights, or freedoms of the data subject. There is no set way in which controller have to do this, but it is important that they record their reasoning in some way, to show that an **appropriate decision-making process** was utilised to justify processing, and that data **subject rights and freedoms were sufficiently taken into account**. The results of this assessment should also be reviewed if there is a significant change in the nature or context of the processing operations.

Further Processing

Although the principle of **'purpose limitation'**, set out in Article 5(1)(b) GDPR, does require that personal data are collected for 'specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes', there are limited cases in which 'further processing' of personal data for purposes other than those for which the personal data were initially collected should be allowed. This is only possible where the **processing is 'compatible'** with the purposes for which the personal data were initially collected.

Article 5(1)(b) GDPR itself even notes that further processing is **not incompatible** with the original purpose where it is for "***archiving*** *purposes in the public interest, scientific or historical* ***research*** *purposes or* ***statistical*** *purposes*", once it is in accordance with Article 89(1) GDPR, which sets out that such further processing must involve appropriate **safeguards** to the data subject's rights and freedoms, including pseudonymisation if appropriate.

Under Article 6(4) GDPR, **certain factors** are set out which a controller must take into account to assess whether a new processing purpose is compatible with the purpose for which the data were initially collected. Where such processing is not based on consent, or on EU or national law relating to matters specified in Article 23 (restrictions relating to the protection of national security, criminal investigations, etc.), controllers should consider the following factors in order to determine whether the further purpose is compatible with the original:

a) any **link** between the original and intended further purposes;

b) the **context** in which the personal data were collected, in particular the **relationship** between the data subject and controller;

c) the **nature** of the personal data, particularly whether they are **sensitive** special category data or concern **criminal** convictions or offences;

d) the possible **consequences** of the intended further processing; and

e) the existence of appropriate **safeguards**, including encryption or pseudonymisation.

However, as alluded to above, where the data subject has given **consent for the further processing** or it is based on law which constitutes a necessary and proportionate measure in a democratic society to safeguard, in particular, important objectives of **general public interest**, the controller should be allowed to further process the personal data irrespective of the compatibility of the purposes.

In any case, controllers are still required to ensure the further processing complies with all of the **rules and principles** set out in the GDPR, particularly the provision of information to the data subject on the purposes of further processing and on their rights, including the right to object.

Law Enforcement Purposes

As mentioned at the outset, certain processing of personal data does not fall under the remit of the GDPR at all, but may instead be covered by the Law Enforcement Directive (LED). The LED deals with the processing of personal data by certain controllers for '**law enforcement purposes**'. The LED is implemented in Irish law through the 2018 Act, primarily through 'Part 5 – Processing of Personal Data for Law Enforcement Purposes', which covers Sections 69-104 of that Act.

Per Section 71(2) of the Act, processing is **lawful and has a legal basis** under the LED where **(a)** it is '**necessary for the performance** of a function of a controller' for one of the purposes mentioned in Section 70, and that function has a **basis in EU or Irish law**; or **(b)** the data subject has given their **consent** to the processing.

There is effectively a **two-step test** to satisfy before controllers can determine whether the processing in question falls under Section 71(2)(a) LED; **firstly**, the controller responsible for the processing in questions must be a 'competent authority' as defined by Section 69 of the Act; but **secondly**, the processing in question must actually be for 'law enforcement purposes', as defined in section 70 of the Act.

Controllers who may be processing personal data for law enforcement purposes need to assess whether the processing they engage in falls under the legal regime of the LED, which only applies in cases where the **controller is a 'competent authority'** (as defined by **Section 69(1)** of the 2018 Act).

This is not limited to processing by bodies who might be typically considered as 'law enforcement authorities' (such as An Garda Síochána), but to any processing for law enforcement purposes, carried out by a public or private body who fits the definition of 'competent authority' (such as local authorities when prosecuting litter fines, or Dublin Bus in relation to ticket offences). The applicability of this regime will need to be assessed on a **case-by-case basis**.

Law enforcement purposes are **defined in section 70 of the 2018 Act** as the processing of personal data where carried out for the purposes of: (i) the **prevention, investigation, detection or prosecution of criminal offences**, including the safeguarding against, and the prevention of, threats to public security; or (ii) the **execution of criminal penalties**.

It is not as simple as presuming that all processing done by law enforcement authorities will fall under the LED regime, or that a private sector entity will not be subject to the LED – in the former case, the law enforcement authority may conduct data processing which has nothing to do with its law enforcement function (HR matters, procurement, etc.), and in the latter case, private sector entities may have been entrusted with public authority or be performing data processing delegated to them by a public authority, where their processing is for law enforcement purposes.